CHAPTER 20

INFORMATION OPERATIONS

INTRODUCTION

In the array of challenges that face an operational attorney today, there is perhaps no more misunderstood, misapplied, mysterious task than that of coordinating the legal aspects of information operations (IO). The debate whether IO add a new dimension to our warfighting capability or represent a revolution that will reshape the way the Army accomplishes its strategic objectives remains unsettled. The National Military Strategy lists IO as one of the key capabilities which the U.S. military must provide in order to give the national leadership a range of viable options for promoting and protecting U.S. interests in peacetime, crisis, and war.[1]

Commentators often shake their heads sagely and intone vague phrases such as "Information operations are the wave of the future." Joint Pub. 3-13 admonishes commanders that "the growth in IO-related technology and capabilities and associated legal issues makes it critical for commanders at all levels of command to involve their staff judge advocates in development of IO policy and conduct of IO."

In practice, IO raise many questions and legal issues that cannot be precisely refined and distilled onto a fact sheet for the curious commander or staff officer. Among other areas, the emerging discipline of IO synthesizes laws and policies related to intelligence collection and oversight, space law, computer security, psychological operations, mission planning, law of armed conflict targeting constraints, information security and exploitation, and search and seizure guidelines. There are many areas where current laws contain gaps, which can frustrate lawyers and commanders who seek crystal clear answers for important operational issues. Despite the somewhat shadowy framework of law and practice, IO have a stature and following that will make them integral to future operational planning and execution.

OLD WINE INTO NEW WINESKINS

In a very real sense, IO is nothing new. No commander in history has willingly communicated his intentions to the enemy, or intentionally followed the enemy deception plan. History is filled with examples of successful IO. The D-Day deception showed the power of giving the enemy a false impression. The Union fortune in finding Lee's plans prior to the Battle of Antietam shows the need to preserve one's own information. The intelligence community as a whole is built around the need for preserving information vital to national security while learning the information crucial to our adversaries.

FORMAL DEFINITIONS

IO consists of actions taken to affect adversary information and information systems while defending our own information. IO are conducted at all levels of war (strategic, operational, and tactical) and across the full range of military operations (peacetime, conflict, and war). Thus, IO is an umbrella term that includes what used to be regarded as distinct facets of operations into one overarching planning and execution imperative. The operational component of IO has seven elements:

- Operations Security (OPSEC) - The discipline relating to denying valuable tactical and strategic information to the enemy.[2]
- Psychological Operations (PSYOP) - The art of shaping enemy perceptions in order to achieve the objectives of the mission. Current law and policy prohibits PSYOP directed at a U.S. target audience.[3]

---

[1] http://www.dtic.mil/jcs/nms.

[2] *See* JOINT PUB. 3-54, JOINT DOCTRINE FOR OPERATIONS SECURITY (27 Jan. 1996).

[3] *See* THE JOINT CHIEFS OF STAFF, JOINT PUB. 3-53, DOCTRINE FOR JOINT PSYCHOLOGICAL OPERATIONS (10 July 1996). PSYOP are operations planned to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.

- Electronic Warfare (EW) - The use of high powered microwaves to jam enemy transmissions or use technology to interfere with the enemy's ability to collect and transmit information. The goal is to degrade, disrupt, deny, and exploit the enemy use of the electromagnetic spectrum.
- Military Deception – A key part of successful operations predating the Trojan Horse. This is an important element in obtaining tactical or operational surprise.
- Physical Destruction – Using kinetic ordinance to target the enemy ability to collect or transmit information. Despite the objections of some journalists who are often using enemy infrastructure for their own commercial purposes, enemy radio towers, communications stations, power grids, etc. are lawful military targets so long as planners and lawyers consider the familiar targeting principles in reviewing the target packet and approving the target. A good example is the destruction of the Serbian television station in Belgrade that was broadcasting propaganda and misinformation to the civilians and military in the Former Republic of Yugoslavia. The key is to articulate the military necessity for attacking the target and do so in a manner that minimizes collateral damage.

Space is used for military communications, command and control, navigation, and weapons guidance. IO planners often encounter questions regarding the legal extent to which satellites can be targeted. Orbital surveillance is legal and common.[4] Many IO activities would clearly be permissible within the parameters of the "peaceful use" required by the relevant treaties. There are several major international agreements that relate to the legality of targeting orbital objects.

1) The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies.[5] This Treaty mandates that all nations are free to explore and use Outer Space on a basis of equality and in accordance with international law, to include the United Nations Charter. **NOTE**: This allows a wide range of IO activities which are characterized as either under the authority of the Security Council or are taken pursuant to the rights of individual or collective self defense contained in the Charter.

2) The 1971 Agreement Relating to the International Telecommunications Satellite Organization (INTELSAT)[6] and The 1976 Convention on the International Maritime Satellite Organization (INMARSAT)[7] require that space be used for "other than for military purposes" and "peaceful purposes" respectively. State practice has established that these conventions are relevant to IO only because they establish the principle of nondiscrimination among states that use satellites.[8]

THE BOTTOM LINE: Satellites that contribute to enemy military action are lawful targets so long as the damage caused by either destroying satellite or interfering with its efficient transmission of information does not cause damage to civilian targets that is excessive in relation to the direct and concrete military advantage to be gained. For example, a GPS satellite that transmits information to a fleet of civilian airliners while they are in flight might not be a lawful target.

- Civil Affairs (CA) – The Civil-Military Commission is one of the most important facets of the complicated operation in Bosnia. The CA function is to spread information to the population, civilian police, local officials, host nations businesses, NGOs, etc. Successful CA gain local acceptance and support for the military goals. The CA effort is a force multiplier because it offers the prospect for accomplishing the military mission without having to apply military power.[9] The nature of the CA mission puts personnel in a very favorable position to collect information. CA activities encompass the entire range of cultural, political, social, and economic issues within the area of operations. The CA unit should be included within the intelligence collection plan and should be of great use in planning the PSYOP campaign themes and target audience.
- Public Affairs (PA) – The media can be a powerful ally in disseminating truthful information regarding U.S. objectives and practices. In particular, the media war can be decisive in determining whether or not the U.S. and its

[4] Glenn H. Reynolds, *International Space Law: Into the Twenty-First Century*, 25 VAND. J. TRANSNAT'L L. 225, 230 (1992).

[5] 18 U.S.T. 2410, T.I.A.S. No. 6347, 610 U.N.T.S. 205 (27 Jan. 1967).

[6] 23 U.S.T. 3813, T.I.A.S. No. 7532 (20 Aug. 1971), *reprinted in* 10 I.L.M. 909 (1971).

[7] 31 U.S.T. 1, T.I.A.S. No. 9605, 1143 U.N.T.S. 105 (3 Sept. 1976).

[8] LAWRENCE T. GREENBERG ET AL, INFORMATION WARFARE AND INTERNATIONAL LAW 22 (1998).

[9] *See* JOINT PUB. 3-57, JOINT DOCTRINE FOR CIVIL AFFAIRS (31 MAY 1996).

allies achieve the objectives of the operation.[10] The role of PA as a component of the broader IO effort is to counter enemy propaganda and protect from misinformation and rumors. PA provides objective reporting which is accurate, truthful, and balanced, yet which is conscious of the OPSEC requirements for protecting vital military information.

At its root, the emerging doctrine and practice of information operations is best understood as an element of combat power which should be focused when and where it best supports the operation. For example, the information campaign to prevent widespread violence following the Brcko decision in Bosnia-Herzegovina began more than a year before the decision was released. In this sense, IO are driven by the planning factors of METT-TC just as any other aspect of combat power (e.g. mission, enemy, terrain, troops, time available, and civilian considerations).

Offensive IO are those operations undertaken to influence the human decision making processes of the adversary**.** Offensive IO involves the integration and orchestration of varied activities into a coherent, seamless plan to achieve specific objectives. Offensive IO objectives must be clearly established, support overall national and military objectives, and include identifiable indicators of success.

In order to efficiently attack adversary information and information systems, planners must be able to do the following:

- Understand the adversary's or potential adversary's perspective and how it may be influenced by IO
- Establish IO objectives
- Identify information systems value, use, flow of information, and vulnerabilities
- Identify targets that can help achieve IO objectives
- Determine the target set
- Determine the most effective IO capabilities for affecting the vulnerable portion of the targeted information or information systems
- Predict the consequences of employing specific IO capabilities with a predetermined level of confidence.

Defensive IO[11] integrate and coordinate policies and procedures, operations, personnel, and technology to protect information and defend information and information systems. Defensive IO are conducted and assisted through information assurance (IA), OPSEC, physical security, counterdeception, counter- PSYOP propaganda, counterintelligence (CI), EW. Defensive IO ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes.

"Special information operations" (SIO) are information operations that, by their sensitive nature and due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process.[12] This class of IO may require the additional coordination mandated by Title V of the National Security Act.

THE PROBLEM OF PLANNING

Current doctrine calls for an IO cell which has the responsibility of coordinating, deconflicting, and orchestrating the whole range of discrete functions that together comprise the IO plan. For example, since the PSYOP campaign will transmit information to enemy intelligence systems, it must be coordinated with the CI, deception, and OPSEC planners. Likewise, proper planning will prevent the EW assets from nullifying the efforts of the PA, CA, or PSYOP elements.

---

[10] *See* JOINT PUB. 3-67, DOCTRINE FOR PUBLIC AFFAIRS IN JOINT OPERATIONS (14 MAY 1997).

[11] *See generally* CHAIRMAN, JOINT CHIEFS OF STAFF INSTR. 6510.01B, DEFENSIVE INFORMATION OPERATIONS IMPLEMENTATION (22 Aug. 1997).

[12] This class of information operations may, by definition, fall within the realm of covert action as defined in 50 U.S.C. § 413 (any activity or activities of the U.S. government designed to influence political, economic, or military conditions abroad, where it is intended that the role of the U.S. government will not be apparent or acknowledged publicly). 50 U.S.C. § 413b(f) prohibits any covert action which is "intended to influence United States political processes, public opinion, policies, or media." Title V of the National Security Act requires specific presidential findings prior to the initiation of a covert action, and mandates that the President keep the Congressional Intelligence committees "fully and currently informed."

Joint Pub. 3-13 and Army doctrine both call for the IO cell to include the JAG, the signal officer, the EW, deception, PSYOP, and OPSEC representatives, as well as the J-2 and targeting representatives from the J-3. A field support team (FST) from the Land Information Warfare Activity (LIWA) can augment the IO cell (which can be found at all levels of command).[13] A Joint Task Force IO cell may be augmented by a team from the Joint Command and Control Warfare Center. Not surprisingly, given the range of activities that are part of the IO plan, the relevant information is found in various places within the OPLAN.

In a plan following the JOPES format, Appendix 3, to Annex C has recently been redesignated as the IW (Information Warfare) appendix. The IW appendix has the following subsections:

Tab A Military Deception

Tab B Electronic Warfare

Tab C Operations Security

Tab D Psychological Operations

Tab E Physical Destruction

Aside from these specific locations for IO related areas, the Civil Affairs annex (Annex G) is a crucial component of the IO planning. The Public Affairs Annex (Annex F) must be integrated as well. Finally, the two specific references to IO are found in Appendix 2 (IO-D) to Annex K (C3) and Appendix 6 to Annex B (Intel Spt to IO).

THE IO PLANNING PROCESS USING MILITARY DECISION-MAKING PROCESS (MDMP)

The members of the IO cell should follow the **MDMP** in preparing an OPLAN. At the ***Receipt of Mission*** phase, the IO team must be focused with the rest of the battle staff on defining a clearly stated mission. The commander's vision should include IO specific guidance on how the IO cell should support the operation. The IO planners should state the mission in finite and measurable terms, and the components of the IO plan should be tied directly to the operational decision points specified in the commander's intent.

During the ***Mission Analysis*** phase of planning, the IO cell should develop a concept that is linked to the overall mission. The IO concept is a who, what, where, when, why, and how articulation of the IO activities that will support the specified and implied tasks developed by the battle staff. Although the initial set of IO objectives is defined during mission analysis, it will be refined further during COA development.

During the ***Course of Action (COA) Development***, the IO cell should coordinate IO actions with the planning scheme. For example, the IO team will succinctly state how IO will support the operation, plan IO execution timelines, and develop IO Target and Protect lists. The ***COA Analysis (Wargame)*** phase of planning will entail comparison of the IO synchronization matrix with the overall battle staff sync matrix. For example, timing a deep Apache attack against a high-value C4I (Command, Control, Communications, Computers, Intelligence) node to coincide with a suppression of enemy air defense (SEAD) mission may significantly aid the IO campaign.

The ***COA Comparison*** will require the IO cell to weigh the strengths and weaknesses of IO support for each of the COA developed by the battle staff. The IO staff will brief the IO aspects of the plan to the commander prior to ***COA Approval.*** The IO annex developed during ***Orders Production*** must focus on providing the relevant information for both offensive and defensive IO. IO input to the base order is generally included in paragraph 3 (operations), but the IO planners must ensure that information is cross-walked between the various annexes that touch on IO related subjects.

[13] To request LIWA assistance, Army organizations should address messages and correspondence to one of the following: DAMO-ODI, (703) 697-1119/3636, DSN 227, HQDA, ATTN: DAMO-ODI, 400 Army Pentagon, Washington, D.C. 20310-0400, GENSER HQDAWASHDC//DAMO-ODI//, NIPRNET fredrib@hqda-aoc.army.pentagon.mil

THE NEW DIMENSION

The explosion of technology has given military planners an important new dimension for managing and interdicting information. In this new arena, the electrons are the weapons. While the underlying notion of IO is as old as war itself, the speed with which information flows is indeed revolutionary. At the same time, the military is now dependent upon the information stored in computer systems around the world, and relies on the accurate transmission of information.

In the realm of offensive IO, the computer revolution has spawned a new doctrinal term. CNA is a new acronym for **computer network attack. CNA entails** operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. **(**NOTE: This term was promulgated in DoDD S-3600.1 of 9 Dec 96.)

IO AND THE LAW OF WAR

The revolution in computer technology and the interconnected flow of information between sovereign states presents new challenges for conducting IO as a lawful component of military operations. The principles of the Law of War certainly apply, but with a couple of minor exceptions, the black letter law does not fit cleanly into an IO application.

The interconnected nature of the digital age raises issues relating to the **Law of Neutrality**[14] in any IO campaign. As a general rule, all acts of hostility in neutral territory, including neutral lands, waters, and airspace are prohibited. In theory, using the wires or digital cables of a network associated with a neutral Party as a conduit for information operations would jeopardize that State's neutrality. If the neutral nation is unable or unwilling to affirmatively maintain its neutrality, the belligerents are allowed to take such measures as are necessary to negate the enemy efforts.[15] There are some specific IO related prohibitions with regard to neutral States.

- Hague V, Art. 3 forbids a belligerent from erecting a "wireless telegraphy station or other apparatus for the purpose of communicating" on the territory of the neutral, and forbids belligerents from using "any installation of this kind established by them before the war … for purely military purposes." (emphasis added)

- Art. 5 mandates that the neutral state prevent any belligerent from allowing belligerents to establish communications equipment on its territory, in its airspace, or in its waters.

- Lawful Activities with IO Implications. Hague V, Art. 8 mandates that a neutral power is not required to "forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals"

THE PROBLEM OF UNANTICIPATED CONSEQUENCES:[16]

IO planners should consider the problems of discriminating between civilian and military targets when designing a CNA. Protocol I, Art. 48 mandates that Parties to the conflict distinguish between the civilian population and combatants at all times, and between civilian objects and military objectives, and direct operations only against military objectives. An EW objective could likely knock out civilian ambulance radios, for example. Planners must bear in mind the fundamental principles of the Law of War:

- Protocol I, Art. 51(2) "The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited."

---

[14] *See* Hague Convention No. V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, 36 Stat. 2310, UST 540.

[15] CENTER FOR OCEANS LAW AND POLICY, ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS ¶ 7.3 (15 Nov. 1997).

[16] *See, e.g.*, Protocol I, Annex I, arts. 7-13.

- Hague IV, Art. 22 "The right of belligerents to adopt means of injuring the enemy is not unlimited."

- Protocol I, Art. 57(2)(a)(ii), those who plan or decide upon attack shall "take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event, to minimizing, incidental loss of civilian life, injury to civilians, and damage to civilian objects."

- Protocol I, Art. 51(5)(b): Where civilian objects are not specifically targeted but nonetheless are at risk because of collateral damage, the collateral damage may not be excessive in relation to the direct and concrete military advantage obtained through the destruction of the intended target.

Perfidy versus Lawful Deception: Protocol I, Art. 37 prohibits belligerents from killing, injuring, or capturing an adversary by perfidy. The essence of this offense lies in acts designed to gain advantage by falsely convincing the adversary that applicable rules of international law prevent engaging the target when in fact they do not. The use of enemy codes and signals is a time-honored means of tactical deception. However, misuse of distress signals or of signals exclusively reserved for the use of medical aircraft would be perfidious.[17] The use of deception measures to thwart precision guided munitions would be allowed, while falsely convincing the enemy not to attack a military target by electronic evidence that it was a hospital would be perfidious.

STATUTORY TOOLS FOR DEFENSIVE IO

The computer age has spawned many statutes that will be the tools used by the operational lawyer to assist the **IO** cell in conducting defensive IO. Some of these are summarized below.

➔ **Electronic Communications Privacy Act of 1986 (ECPA)**.[18] Enacted 18 U.S.C. §§ 2701-11, §§ 3121-27, § 1367, § 3117, § 2521, and made numerous amendments to provisions of the Communications Act of 1934.

§ 107 of the Act specifically states that "Nothing contained … constitutes authority for the conduct of any intelligence activity."[19] 18 U.S.C. § 2511 makes it unlawful

> for "any person" to "intentionally intercept, use, or disclose or endeavor to intercept, use, or disclose any wire, oral, or electronic communication." **NOTE:** Must distinguish between real-time interception which is governed by 18 U.S.C. § 2511 and stored communications such as e-mail that is governed by 18 U.S.C. § 2703. The ECPA lists 9 Statutory Exceptions, 3 of which are central to IO because they permit monitoring by:
>
> > 1) The System Administrator "while engaged in any activity which is necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service." 18 U.S.C. § 2511(2)(a)(i)
> >
> > 2) "where such person is a party to the communication or one of the parties has given consent to such interception." 18 U.S.C. § 2511(2)(c)

[17] Protocol I, Art. 38(1).

[18] Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[19] The Foreign Intelligence Surveillance Act of 1978 (FISA) is the vehicle for defensive IO aimed at discovering the loss of **FOREIGN INTELLIGENCE INFORMATION**; Information that relates to the ability of the U.S. to protect against the following: Attack or hostile act of a foreign power or agent, Sabotage or international terrorism, Clandestine intelligence activities by an intelligence network or service of a foreign power or by an agent, or Information on foreign power or foreign territory relative and necessary to the national defense and security of the U.S. or the foreign affairs of the U.S.

FISA is the statutory mechanism for obtaining two major categories of information related to defensive IO:

Acquisition of a "nonpublic communication" by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of the communication.

Physical searches seeking to obtain foreign intelligence information.

or 3) pursuant to a court order directing such assistance signed by the authorizing judge or a certification in writing by a person designated in 18 U.S.C. § 2518(7) or the Attorney General that no court order is required by law and that all statutory requirements have been met. 18 U.S.C. § 2511(2)(a)(ii)

➔Information Operations Warrants for Law Enforcement Purposes.

- 18 U.S.C. § 2703(c): with subpoena, the government can obtain the name, address, local and long distance telephone billing records, telephone number or other subscriber information. The government entity receiving such information is not required to provide notice to the consumer.

- 18 U.S.C. § 2703(d) allows a court to issue an order for disclosure if the government offers specific and articulable facts that there are reasonable grounds to believe that the contents of electronic communication or the records within the service provider's database or other information sought are relevant and material to an ongoing criminal investigation.

- The service provider may move to quash or modify the order if the request is unusually voluminous or would cause an undue burden on the carrier.

- § 270 is the mechanism for obtaining subscriber connection logs, sending IP addresses, receiving IP addresses, times of access and log on, content of saved communications, and more.

COMSEC Monitoring: This is a clearly defined, bright line exception to the general limitations on content monitoring. § 107(b)(1) of the Electronic Communications Privacy Act specifically allows activities intended to "intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes."

NSA is the proponent under the National Telecommunications and Information Systems Security Directive (NTISS) Directive No. 600, Communications Security Monitoring.

COMSEC is one of the tools available to fulfill the DoD mandate to accredit automated information systems and ensure "compliance with automated information systems security requirements."[20] COMSEC monitoring as part of the IO campaign is permitted by revised AR 380-53.[21] Here are some of the key guidelines for conducting COMSEC:

- Information Systems Security Monitoring will be conducted only in support of security objectives.

- Information Systems Security Monitoring will not be performed to support law enforcement or criminal or counterintelligence investigations.

- The results of Information Systems Security Monitoring shall not be used to produce foreign intelligence or counterintelligence, as defined in Executive Order 12333.

The NTISS (as implemented in AR 380-53) requires that the persons conducting Information Systems Monitoring receive formal training in the procedures outlined in AR 380-53, the provisions of AR 381-10, the provisions of AR 381-12, para. 3-1, the provisions of AR 190-53, and the provisions of applicable Federal laws (18 U.S.C. § 2510, etc.)

These are the prerequisites for lawful Information Systems Monitoring:

NOTIFICATION: Users of official DOD telecommunications will be given notice that: (1) Passing classified information over non-secure DOD telecommunications systems, other than protected distribution systems or automated

[20] U.S. DEP'T OF DEFENSE, DIR. 5200.28, SECURITY REQUIREMENTS FOR AUTOMATED INFORMATION SYSTEMS (21 Mar. 1998).

[21] U.S. DEP'T OF ARMY, FIELD MANUAL 380-53, INFORMATION SYSTEMS SECURITY MONITORING (29 Apr. 1998). <http://www.acert.belvoir.army.mil/ar380_53.pdf>

information systems accredited for classified processing is prohibited; (2) Official DOD telecommunications systems are subject to Information Systems Security Monitoring at all times; and (3) Use of official DOD telecommunications systems constitutes consent by the user to Information Systems Security Monitoring at any time.

CERTIFICATION: The Office of the General Counsel has certified the adequacy of the notification procedures in effect, and the OGC and TJAG have given favorable legal review of any proposed Information Systems Security Monitoring that is not based on a MACOM request. *See* para. AR 380-53, 2-4 for a specific list of information required prior to certification.

AUTHORIZATION: The Deputy Chief of Staff for Intelligence has authorized Information Systems Security Monitoring to be conducted within the MACOM involved.

Notification Guidance for Automated Information Systems

Use of Information Acquired During Information Systems Security Monitoring. See AR 380-53, para. 2-8(c)(3) for required procedures if materials are required as evidence.

The results of Information Systems Security Monitoring may not be used in a criminal prosecution without prior consultation with the OGC and TJAG. (AR 380-53, para. 2-8(5)).

Information obtained through Information Systems Security Monitoring may be used in connection with disciplinary or administrative action against Department of the Army personnel for knowing, willful, or negligent actions that result in the unauthorized disclosure of classified information (*see* AR 380-5, paras 14-101 and 14-102). In this case, the Information Systems Security Monitoring element is authorized to release names, or recorded media, of the telecommunications involved to the supported commander or designated representative for use as evidence. Procedures will be strictly adhered to as follows:

- The supported commander, after having consulted with the servicing judge advocate (JA), will provide the Information Systems Security Monitoring element with a written request, specifically identifying the telecommunications messages or communications required. The request will identify the servicing JA consulted.

- The Information Systems Security Monitoring element will obtain a signed receipt from the supported commander or designated representative for the requested materials. The receipt will include a statement that the commander or representative is familiar with and will comply with the security requirements and privacy restrictions applicable to the material.

- The Information Systems Security Monitoring element will immediately notify its chain of command that the material has been requested .

- The Information Systems Security Monitoring unit commander will notify HQDA (DAMI-CHI), in writing, within 5 working days of providing the material to the supported command.

- Information may be obtained incidental to an authorized Information Systems Security Monitoring mission that relates directly to a serious crime such as sabotage or threats or plans to commit offenses that threaten a life or could cause significant damage to or loss of Government property (this includes data on Government AIS).

When evaluating or assessing the security of U.S. Army AIS, Information Systems Security Monitors may detect computer anomalies that could potentially be unauthorized intrusions into Army AIS . When Information Systems Security Monitors detect such anomalies, they must contact the system administrator and ACERT[22] immediately. The system administrator will then follow the procedures of AR 380-19 by taking measures to ascertain that the anomaly is in

[22] The Army Computer Emergency Response Team (ACERT) conducts command and control protect operations in support of the Army to ensure the availability, integrity, and confidentiality of the information and information systems used in planning, directing, coordinating, and controlling forces in the accomplishment of the mission across the full spectrum of support to military operations. *See* < http://www.acert.belvoir.army.mil/> Contact at COMM 1-888-203-6332/ DSN 235-1113.

fact an unauthorized intrusion, notifying counterintelligence (CI) and criminal investigation division (CID) so that the offices may conduct an investigation of the incident.

Information Systems Security Monitors should not support the process of determining if the investigation is properly a law enforcement or intelligence matter, and must discontinue monitoring the suspected intrusion as soon as the system administrator or ACERT has interceded In no case may the Information System Security Monitors continue monitoring the anomaly for more than 24 hours. Data pertaining to the anomaly or suspected intrusion recorded during the 24-hour period will not be accessed until the appropriate legal authorization is obtained to further investigate the activity.